TELEFAX COVER SHEET

PATTERSON & SHERIDAN, LLP
ATTORNEYS AT LAW
595 SHREWSBURY AVENUE
FIRST FLOOR
SHREWSBURY, NJ 07702
TELEPHONE (732) 530-9404
TELEFAX (732) 530-9808

****

THIS TELEFAX MESSAGE IS ADDRESSED TO THE PERSON OR COMPANY LISTED BELOW. IF IT WAS SENT OR RECEIVED INCORRECTLY, OR YOU ARE NOT THE INTENDED RECIPIENT, PLEASE TAKE NOTICE THAT THIS MESSAGE MAY CONTAIN PRIVILEGED OR CONFIDENTIAL MATERIAL, AND YOUR DUE REGARD FOR THIS INFORMATION IS NECESSARY. YOU MAY ARRANGE TO RETURN THIS MATERIAL BY CALLING THE FIRM LISTED ABOVE AT (732) 530-9404

****

THIS MESSAGE HAS 29 PAGES INCLUDING THIS SHEET

TO: Commissioner of Patents

FAX NO.: 571-273-8300

FROM: Kin-Wah Tong

DATE: July 18, 2007

MATTER: Serial No. 10/005,113 Filed: December 5, 2001

DOCKET NO.: ATT/2001-0450

APPLICANT: CARRICO, et al

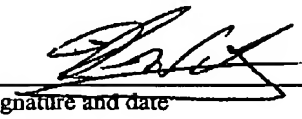
The following has been received in the U.S. Patent and Trademark Office on the date of this facsimile:

___ Request for Extension of time (2 copies)
___ Disclosure Statement & PTO-1449
___ Priority Document
___ Drawings (____ sheets) informal
X APPEAL BRIEF
___ Response to Final Office Action
___ Notice of Appeal Transmittal Letter (2 copy)
X Fee Transmittal (2 copies)
X Deposit Account Transaction
X Facsimile Transmission Certificate dated July 18, 2007
__ _____

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8

I hereby certify that this correspondence is being transmitted by facsimile to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on July 18, 2007, Facsimile No. 571-273-8300

Kin-Wah Tong
Name of person signing this certificate



July 18, 2007
Signature and date

PTO/SB/21 (08-03)

Please type a plus sign (+) inside this box → [+]

Approved for use through 7/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

RECEIVED
CENTRAL FAX CENTER
JUL 18 2007

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/005,113
Filing Date	December 5, 2001
First Named Inventor	CARRICO
Group Art Unit	2136
Examiner Name	David G. Cervetti
Attorney Docket Number	2001-0450

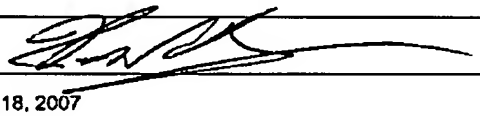
Total Number of Pages in This Submission

ENCLOSURES *(check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Response
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ____
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to Group ***(Appeal Notice, Brief, Reply Brief)***
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) *(please identify below)*:
  Certificate of Facsimile Transmission

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Kin-Wah Tong, Reg. No. 39,400
Signature	
Date	July 18, 2007

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Kin-Wah Tong		
Signature		Date	July 18, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon on the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL for FY 2006

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500

Complete if Known	
Application Number	10/005,113
Filing Date	December 5, 2001
First Named Inventor	CARRICO
Examiner Name	David G. Cervetti
Art Unit	2136
Attorney Docket No.	ATT/2001-0450

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify) : _____

☒ Deposit Account Deposit Account Number: 20-0782 Deposit Account Name: Patterson & Sheridan

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayments of fee(s) Under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee($)	Fee($)	Fee($)	Fee($)	Fee($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	____
Plant	200	100	300	150	160	80	____
Reissue	300	150	500	250	600	300	____
Provisional	200	100	0	0	0	0	____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee($)	Fee Paid ($)
20	-20 or HP= 0	x 50	= ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee($)	Fee Paid ($)
3	- 3 or HP= 0	x 200	= ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims		
	Fee ($)	Fee Paid ($)
	____	____

3. APPLICATION SIZE FEE

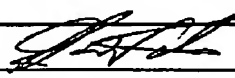
If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
____	- 100 = ____	/ 50 = ____ (round up to a whole number) x		= ____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	____
Other (e.g., late filing surcharge): APPEAL BRIEF	500.00

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	39,400	Telephone	(732) 530-9404
Name (Print/Type)	KIN-WAH TONG			Date	July 18, 2007

PATENT
Atty. Dkt. No. ATT/2001-0450

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:
Sandra Lynn Carrico, et al.

Serial No.: 10/005,113

Confirmation No.: 9439

Filed: December 5, 2001

For: NETWORK SECURITY DEVICE AND METHOD

§ Group Art Unit: 2136

§ Examiner: David Garcia Cervetti

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO, on the date indicated below.

July 18, 2007
Date

Signature

Dear Sir:

APPEAL BRIEF

Appellants submit this Appeal Brief to the Board of Patent Appeals and Interferences on appeal from the decision of the Examiner of Group Art Unit 2136 dated January 18, 2007, finally rejecting claims 1-11. Please charge the fee of $500.00 for filing this brief and all other fees including any extension fees that may be required to make this Brief timely and acceptable to the Patent Office, to Deposit Account No. 20-0782/ATT2001-0450.

07/19/2007 FMETEKI1 00000028 200782 10005113
01 FC:1402 500.00 DA

REAL PARTY IN INTEREST

The real party in interest is AT&T, Corp.

RELATED APPEALS AND INTERFERENCES

The Appellants know of no related appeals or interferences that might directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-11 are pending in the application. Claims 1-11 were originally presented in the application. Claims 1-11 stand rejected in view of the references as discussed below. The rejection of claims 1-11 based on the cited references is appealed. The pending claims are shown in the attached Appendix.

STATUS OF AMENDMENTS

Claims 1-11 were originally filed on December 5, 2001. Amendments to the claims were submitted in the response to the Office Action dated February 7, 2005 filed on May 9, 2005 and the response to the Final Office Action dated July 29, 2005 filed on September 29, 2005. No amendments to the claims, in this application, were submitted subsequent to final rejection. The Appellants are appealing the claims as they read at the time the final rejection dated January 18, 2007 was issued. These claims are shown in the attached Appendix.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides for a security mechanism (10) and method for enabling a user to commence a session between a network peripheral device (12) and a network (14). In an exemplary embodiment of claim 1, the security mechanism (10) comprises an immutable memory element (18) that contains first information including application software that initiates and provides security services (See e.g., Appellants' specification, paragraph [0011]), a persistent memory element (24) that contains second

information to enable the security mechanism to configure the network peripheral device to access different networks (See e.g., Appellants' specification, paragraph [0013]), a volatile memory element (26) that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session (See e.g., Appellants' specification, paragraph [0014]) and a tamper-evident enclosure (32) for enclosing the memory elements (See e.g., Appellants' specification, paragraph [0015]).

In an exemplary embodiment of claim 10, the method comprises accessing an immutable memory element (18) that contains first information that provides security services. (See e.g., Appellants' specification, paragraph [0011].) Then the method accesses a persistent memory element (24) that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access the network. (See e.g., Appellants' specification, paragraph [0013].) Subsequently, the method accesses a volatile memory element (26) that contains third information, including critical data for authentication. (See e.g., Appellants' specification, paragraph [0014].) The method concludes by erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions. (See *Id.*)

In one embodiment, Appellants' invention teaches the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network. For example, a volatile memory element that contains critical data for authentication is erased from the volatile memory at the completion of each connection session. Appellants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (see e.g., Appellants' Specification, paragraphs [0006], and [0013]). In other words, the same device, e.g., a laptop, can be connected to various networks. Once the session is completed with the device, all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See e.g., Appellants' Specification, paragraph [0006].)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-11 stand rejected under 35 U.S.C. §103(a) as being obvious over Sherer, et al. (US Patent 6,115,376, issued September 5, 2000, hereinafter referred to as "Sherer") in view of Jones, et al. (US Patent 5,623,637, issued April 22, 1997, hereinafter referred to as "Jones").

ARGUMENT

1. Claim 1

Claim 1 stands rejected under 35 U.S.C. § 103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

Sherer teaches medium access control address authentication. A network interface card on an end station used in accordance with the invention is disclosed. (See Sherer, col. 5, ll. 32-67.) Notably, the network interface card contains only a single memory module 46. (See *Id.*, emphasis added.)

Jones teaches an encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys. A user in possession of the card enters a password stored in the card's memory. (See Jones, col. 8, ll. 47-67.) If the password is correct, the user has access to needed access codes stored in the password-protected card. (See Jones, col. 9, ll. 1-21.)

The Board's attention is directed to the fact that Sherer and Jones, alone or in any permissible combination, fail to teach, show or suggest a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Appellants' independent claim 1. Specifically, Appellants' independent claim 1 recites:

> 1. A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:
> an immutable memory element that contains first information including application software that initiates and provides security services;
> a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks;

a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and

a tamper-evident enclosure for enclosing the memory elements.

(Emphasis Added)

Appellants' invention teaches the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. Appellants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (See e.g., Appellants' Specification, paragraphs [0006]; and [0013]). In other words, the same device, e.g., a laptop, can be connected to various networks. Once the session is completed all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See e.g., Appellants' Specification, paragraph [0006].)

The alleged combination (as taught by Sherer) fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a immutable memory element, a persistent memory element and a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Appellants' independent claim 1. First, unlike the Appellants' invention that teaches three separate types of memory elements (i.e. immutable memory element, persistent memory element and volatile memory element), Sherer only teaches that the network interface card contains a single memory element 46. (See Sherer, column 5, lines 32-67, FIG. 3, emphasis added.)

However, the Examiner asserts in the Final Office Action and reiterates in the Advisory Action dated May 4, 2007 (hereinafter "Advisory Action"), that the number of memory modules does not determine patentability. (See Final Office Action, page 2, lines 6-13.) Moreover, the Examiner alleges that such limitation would have been obvious because Sherer does explicitly show a program memory module subdivided

into multiple segments or modules in FIG. 3. (See *Id.*) However, the Appellants' argument, as clarified, is that using three different types of memory elements is clearly patentable and not obvious. For example, it is the Appellants' novel combination of using three different types of memory elements, where each of the memory elements is carrying a different type of information, that contributes to the Appellants' novel method for facilitating a secure connection session with a user between a network peripheral device and a network. As discussed above, using three different types of memory elements allows all of the information in the volatile memory element to be erased, thereby preventing re-use of such information by unauthorized users. (See Appellants' Specification, paragraph [0006].)

Moreover, as conceded by the Examiner, Sherer fails to teach or to suggest a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. (See Final Office Action, page 4, lines 1-2.) However, the Examiner alleges that Jones bridges the substantial gap left by Sherer.

The Appellants respectfully submit that Jones fails to bridge the substantial gap left by Sherer because Jones also fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Appellants' independent claim 1. In fact, Jones teaches away from the Appellants' invention because Jones clearly teaches that critical information is stored in the card's memory and fails to teach that this information is erased from the volatile memory at the completion of each connection session. (See Jones, column 8, lines 47-67; column 9, lines 1-21.) Jones specifically teaches that a user supplies a secret password that is written into the smart card I.C. memory. (See Jones, column 8, lines 6-9, emphasis added.) Jones further teaches that ". . . whose processor (i.e. the smart card) is programmed to combine the random number 303 at 325 with the previously stored secret password 301 to form a result value at 327." (See Jones, column 8, lines 21-24, emphasis added.)

Furthermore, the Examiner conceded that Sherer does not expressly disclose third information erased from the volatile memory at the completion of each session. The Examiner then alleged that Sherer suggests using different authentication schemes. Finally, the Examiner then leaps from this alleged suggestion of using different authentication schemes to make obvious the teaching of deleting session keys after the completion of a session. It is respectfully submitted that a general statement such as "using different authentication schemes" would not suggest erasing said third information from the volatile memory at the completion of each connection session. The Examiner provided absolutely no support in the alleged combination of Sherer and Jones for this teaching. In fact, the Examiner is simply using impermissible hindsight.

In rebuttal, the Examiner asserts in the Final Office Action and reiterates in the Advisory Action that the Appellants' arguments with respect the limitation of "erasing the information from the volatile memory at the completion of the session" ignores the fact that one-time passwords were conventional and well known by vaguely citing to Sherer in columns 5-6. (See Final Office Action, page 2, lines 14-20.) However, in doing so, the Examiner contradicts his own concession that Sherer does not expressly disclose such limitation. (See *Id.* at page 4, lines 1-2.)

Regardless, Sherer does not support the Examiner's assertion or interpretation that one-time passwords make obvious the feature of erasing the third information (including critical data for authentication) form the volatile memory at the completion of the session. Sherer explicitly teaches storing critical data for authentication. (See Sherer, column 5, lines 62-67.) Sherer states "[i]n a preferred embodiment, the end station is prevented from reading the secret value stored in the network interface cards, such as by storing it in memory location that is not within the host system address space . . ." (See *Id.*, emphasis added.) In addition, Sherer actually teaches away from the Appellants' invention because Sherer explicitly teaches that the critical data for authentication, such as private key 52, is not contained in a volatile memory element, such as RAM 46. Therefore, Sherer and Jones, alone or in any permissible combination clearly fail to teach or suggest at least the limitation of a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection

session, as positively claimed by Appellants' independent claim 1.

In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. Denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp. 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). It is respectfully submitted that the Examiner failed to present a prima facie case of obviousness. Consequently, the combination of Sherer and Jones clearly falls to render obvious Appellants' invention as recited in independent claim 1. Therefore, the Appellants respectfully submits that claim 1 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

2. Claim 2

Claim 2 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 2 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus,

claim 2 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively, as set forth in claim 2. Performing authentication of the security mechanism itself and the authentication of the user provides added security. Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 2. Therefore, Appellants respectfully submit that claim 2 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

3. Claim 3

Claim 3 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 3 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 3 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection

session, as positively recited by the Appellants' independent claim 1, in combination with wherein the immutable memory contains a private key for encrypting the user and security mechanism identification information, as set forth in claim 3. This ensures that the private keys used by different network peripheral devices remain independent from each other and that the security device cannot be forced to use keys known to an attacker. (See e.g., Appellants' specification, para. [0011].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 3. Therefore, Appellants respectfully submit that claim 3 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

4. Claim 4

Claim 4 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 4 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 4 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the immutable memory comprises a Read-Only Memory (ROM), as set forth in claim 4. (See e.g., Appellants' specification, para. [0011].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 4. Therefore, Appellants respectfully submit that claim 4 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

5. Claim 5

Claim 5 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 5 is also not rendered obvious since the claim depends indirectly from claim 1 and recites additional features of the present invention. Thus, claim 5 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the immutable memory further includes a Write-once ROM, as set forth in claim 5. (See, e.g., Appellants' specification, para. [0012].)

The Examiner uses Official Notice alleging that it would have been obvious to use other types of memory in the device taught by Sherer simply because Sherer teaches using a single type of memory. (See Final Office Action, page 4, line 20 – page 5, line 6.) The Examiner responds by citing to Jones column 5, lines 10-20 as support for the Official Notice. (See Advisory Action dated May 4, 2007, Continuation Sheet, second paragraph.) However, the Appellants respectfully submit that the passage cited by the Examiner to support the Official Notice only teaches the use of RAM, EEPROM and read-only memory. Jones does not teach or suggest the use of Write-Once ROM in combination with the other types of memory as claimed by the Appellants' dependent claim 5. Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 5. Therefore, Appellants respectfully submit that claim 5 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

6. Claim 6

Claim 6 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 6 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 6 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the persistent memory comprises at least one of one of a Complementary Metal Oxide Semiconductor Random Access Memory (CMOSRAM) and a Programmable Read Only Memory (PROM), as set forth in claim 6. Advantageously, the PROM stores configuration data that enables the security mechanism to facilitate a connection with different networks. (See, e.g., Appellants' specification, para. [0013].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 6. Therefore, Appellants respectfully submit that claim 6 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

7. Claim 7

Claim 7 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones

does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 7 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 7 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the volatile memory comprises a random access memory, as set forth in claim 7. Advantageously, all data within the RAM may be erased and only remains for the duration of a session. (See e.g., Appellants' specification, para. [0014].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 7. Therefore, Appellants respectfully submit that claim 7 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

8. Claim 8

Claim 8 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 8 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 8 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory

element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the tamper evident enclosure readily exhibits any attempt to gain access there through to the memory elements enclosed therein, as set forth in claim 8. Advantageously, a user who inspects the tamper-evident enclosure can easily observe whether anyone has attempted to gain access to any of the Security ROM, Write-Once ROM, Configuration memory or volatile memory. (See e.g., Appellants' specification, para. [0015].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 8. Therefore, Appellants respectfully submit that claim 8 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

9. Claim 9

Claim 9 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 1. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 1, dependent claim 9 is also not rendered obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 9 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively recited by the Appellants' independent claim 1, in combination with wherein the physical security of the security mechanism depends on the degree of tamper resistance of the enclosure, as set forth in claim 9. Thus, the effective level of the physical security may depend on the selection of the materials and fabrication

technology employed. (See e.g., Appellants' specification, para. [0015].) Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 9. Therefore, Appellants respectfully submit that claim 9 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

10. Claim 10

Claim 10 stands rejected under 35 U.S.C. § 103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

Sherer teaches medium access control address authentication. A network interface card on an end station used in accordance with the invention is disclosed. (See Sherer, column 5, lines 32-67.) Notably, the network interface card contains only a single memory module 46. (See *Id.*, emphasis added.)

Jones teaches an encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys. A user in possession of the card enters a password stored in the card's memory. (See Jones, column 8, lines 47-67.) If the password is correct, the user has access to needed access codes stored in the password-protected card. (See Jones, column 9, lines 1-21.)

The Board's attention is directed to the fact that Sherer and Jones, alone or in any permissible combination, fail to teach, show or suggest a method for facilitating a secure connection session with a user between a network peripheral device and a network comprising erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions, as positively claimed by Appellants' independent claim 10. Specifically, Appellants' independent claim 10 recites:

> 10. A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:
> accessing an immutable memory element that contains first information that provides security services;
> accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access a network;
> accessing a volatile memory element that contains third information, including the critical data for authentication; and
> erasing said third information not later than the end of the connection

session so no third information remains in the volatile memory between sessions. (Emphasis Added)

In an exemplary embodiment, the Appellants' invention teaches the novel concept of a method for facilitating a secure connection session with a user between a network peripheral device and a network comprising erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions. Appellants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (See e.g., Appellants' Specification, paragraphs [0006] and [0013]). In other words, the same device, e.g., a laptop, can be connected to various networks. Once the session is completed all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See e.g., Appellants' Specification, paragraph [0006].)

The alleged combination (as taught by Sherer) fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a immutable memory element, a persistent memory element and a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Appellants' independent claim 10. First, unlike the Appellants' invention that teaches three separate types of memory elements (i.e. immutable memory element, persistent memory element and volatile memory element), Sherer only teaches that the network interface card contains a single memory element 46. (See Sherer, column 5, lines 32-67, FIG. 3, emphasis added.)

However, the Examiner asserts in the Final Office Action and reiterates in the Advisory Action dated May 4, 2007 (hereinafter "Advisory Action"), that the number of memory modules does not determine patentability. (See Final Office Action, page 2, lines 6-13.) Moreover, the Examiner alleges that such limitation would have been obvious because Sherer does explicitly show a program memory module subdivided into multiple segments or modules in FIG. 3. (See *Id.*) However, the Appellants' argument, as clarified, is that using three different types of memory elements is clearly

patentable and not obvious. For example, it is the Appellants' novel combination of using three different types of memory elements, where each of the memory elements is carrying a different type of information, that contributes to the Appellants' novel method for facilitating a secure connection session with a user between a network peripheral device and a network. As discussed above, this allows all of the information in the volatile memory element to be erased, thereby preventing re-use of such information by unauthorized users. (See e.g., Appellants' Specification, paragraph [0006].)

Moreover, as conceded by the Examiner, Sherer fails to teach or to suggest erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions. (See Final Office Action, page 4, lines 1-2.) However, the Examiner alleges that Jones bridges the substantial gap left by Sherer.

The Appellants respectfully submit that Jones fails to bridge the substantial gap left by Sherer because Jones also fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions, as positively claimed by Appellants' independent claim 10. In fact, Jones teaches away from the Appellants' invention because Jones clearly teaches that critical information is stored in the card's memory and fails to teach that this information is erased from the volatile memory at the completion of each connection session. (See Jones, column 8, lines 47-67; column 9, lines 1-21.) Jones specifically teaches that a user supplies a secret password that is written into the smart card I.C. memory. (See Jones, column 8, lines 6-9, emphasis added.) Jones further teaches that ". . . whose processor (i.e. the smart card) is programmed to combine the random number 303 at 325 with the previously stored secret password 301 to form a result value at 327." (See Jones, column 8, lines 21-24, emphasis added.)

Furthermore, the Examiner conceded that Sherer does not expressly disclose third information erased from the volatile memory at the completion of each session. The Examiner then alleged that Sherer suggests using different authentication schemes. Finally, the Examiner then leaps from this alleged suggestion of using

different authentication schemes to make obvious the teaching of deleting session keys after the completion of a session. It is respectfully submitted that a general statement such as "using different authentication schemes" would not suggest erasing said third information from the volatile memory at the completion of each connection session. The Examiner provided absolutely no support in the alleged combination of Sherer and Jones for this teaching. In fact, the Examiner is simply using impermissible hindsight.

In rebuttal, the Examiner asserts in the Final Office Action and reiterates in the Advisory Action that the Appellants' arguments with respect the limitation of "erasing the information from the volatile memory at the completion of the session" ignores the fact that one-time passwords were conventional and well known by vaguely citing to Sherer in columns 5-6. (See Final Office Action, page 2, lines 14-20.) However, in doing so, the Examiner contradicts his own concession that Sherer does not expressly disclose such limitation. (See *Id.* at page 4, lines 1-2.)

Regardless, Sherer does not support the Examiner's assertion or interpretation that one-time passwords make obvious the feature of erasing the third information (including critical data for authentication) form the volatile memory at the completion of the session. Sherer explicitly teaches storing critical data for authentication. (See Sherer, column 5, lines 62-67.) Sherer states "[i]n a preferred embodiment, the end station is prevented from reading the secret value stored in the network interface cards, such as by storing it in memory location that is not within the host system address space . . ." (See *Id.*, emphasis added.) In addition, Sherer actually teaches away from the Appellants' invention because Sherer explicitly teaches that the critical data for authentication, such as private key 52, is not contained in a volatile memory element, such as RAM 46. Therefore, Sherer and Jones, alone or in any permissible combination clearly fail to teach or suggest at least the limitation of erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions, as positively claimed by Appellants' independent claim 10.

In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. See In re Fine, 837 F.2d 1071, 1073, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In so doing, the

Examiner is expected to make the factual determinations set forth in Graham v. John Deere Co., 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir.), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. Denied, 475 U.S. 1017 (1986); ACS Hosp. Sys., Inc. v. Montefiore Hosp. 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness. Note In re Oetiker, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). It is respectfully submitted that the Examiner failed to present a prima facie case of obviousness. Consequently, the combination of Sherer and Jones clearly fails to render obvious Appellants' invention as recited in independent claim 10. Therefore, the Appellants respectfully submits that claim 10 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

11. Claim 11

Claim 11 stands rejected under 35 U.S.C. §103 as being unpatentable over Sherer in view of Jones. Appellants respectfully traverse the rejection.

The Appellants submit that Sherer in view of Jones does not teach, show, or suggest all of the limitations of independent claim 10. Since Sherer in view of Jones does not render obvious Appellants' invention as recited in Appellants' independent claim 10, dependent claim 11 is also not rendered obvious since the claim depends directly from claim 10 and recites additional features of the present invention. Thus, claim 11 should be deemed patentable for at least the reasons stated above with respect to independent claim 10.

Secondly, the Appellants contend that Sherer in view of Jones does not teach the novel concept of a method for facilitating a secure connection session with a user

between a network peripheral device and a network comprising erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions, as positively recited by the Appellants' independent claim 10, in combination with wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively, as set forth in claim 11. Performing authentication of the security mechanism itself and the authentication of the user provides added security. Thus, Sherer in view of Jones clearly fails to render obvious Appellants' dependent claim 11. Therefore, Appellants respectfully submit that claim 11 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

CONCLUSION

For the reasons advanced above, the Appellants respectfully urge that the rejections of claims 1-11 as being unpatentable under 35 U.S.C. § 103 are improper. Reversal of the rejections in this appeal is respectfully requested. If necessary, please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 20-0782/ATT/2001-0450, and please credit any excess fees to the above referenced deposit account.

Respectfully submitted,

July 18, 2007

Kin-Wah Tong
Attorney Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Suite 100
Shrewsbury, NJ 07702

CLAIMS APPENDIX

1. (Previously Presented) A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:

an immutable memory element that contains first information including application software that initiates and provides security services;

a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks;

a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and

a tamper-evident enclosure for enclosing the memory elements.

2. (Previously presented) The security mechanism according to claim 1 wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively.

3. (Original) The security mechanism according to claim 1 wherein the immutable memory contains a private key for encrypting the user and security mechanism identification information.

4. (Original) The security mechanism according to claim 1 wherein the immutable memory comprises a Read-Only Memory (ROM).

5. (Original) The security mechanism according to claim 4 wherein the immutable memory further includes a Write-once ROM.

6. (Previously presented) The security mechanism according to claim 1 wherein the persistent memory comprises at least one of one of a Complementary Metal Oxide Semiconductor Random Access Memory (CMOSRAM) and a Programmable Read Only

Memory (PROM).

7. (Original) The security mechanism according to claim 1 wherein the volatile memory comprises a random access memory.

8. (Original) The security mechanism according to claim 1 wherein the tamper evident enclosure readily exhibits any attempt to gain access there through to the memory elements enclosed therein.

9. (Original) The security mechanism according to claim 1 wherein the physical security of the security mechanism depends on the degree of tamper resistance of the enclosure.

10. (Previously Presented) A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:

accessing an immutable memory element that contains first information that provides security services;

accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access the network;

accessing a volatile memory element that contains third information, including critical data for authentication; and

erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions.

11. (Original) The method according to claim 10 wherein the security services include authentication of the security mechanism itself and authentication of the user to the network upon receipt of identification information from the security mechanism and the user, respectively.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None